CLAIMS

What is claimed is:

1. A chaos privacy system for use in communicating an analog signal, the system comprising:

a transmitter comprising:

a key stream generator comprising a chaotic circuit that generates a key stream in response to a private key parameter, and transmits a key synchronization parameter; and

a transmitting chaotic circuit that processes the analog information signal and the key stream to generate and transmit a cipherwave; and

a receiver, for receiving the transmitted cipherwave, the transmitted key synchronization parameter, and a copy of the private key parameter, that comprises:

a key stream generator comprising a chaotic circuit that processes the copy of the private key parameter and the transmitted key synchronization parameter to generate a copy of the key stream; and

a receiving chaotic circuit that processes the copy of the key stream and the cipherwave to demodulate the cipherwave to recover and output the information signal.

2. The system recited in Claim 1 wherein the key stream generator in the transmitter comprises:

a first chaotic circuit comprising a first sample and hold circuit coupled to a first voltage controlled oscillator; and

a second chaotic circuit comprising a second sample and hold circuit coupled to a second voltage controlled oscillator;

wherein an output of the first voltage controlled oscillator provides an input to the second sample and hold circuit, a first output of the second voltage controlled oscillator provides an input to the first sample and hold circuit, the first voltage controlled oscillator outputs the key stream, and a second output of the second voltage controlled oscillator outputs the key synchronization parameter.

3. The system recited in Claim 2 wherein the transmitting chaotic circuit comprises:

a hard limiting circuit for receiving the key stream from the key stream generator and for converting the output of the first voltage controlled oscillator to selected fixed values; and

an analog multiplier circuit for multiplying the information signal with the sampled random signal to produce the cipherwave.

4. The system recited in Claim 1 wherein the key stream generator in the receiver comprises:

a third chaotic circuit comprising a third sample and hold circuit coupled to a third voltage controlled oscillator; and

a fourth chaotic circuit comprising a fourth sample and hold circuit coupled to a fourth voltage controlled oscillator;

wherein the key synchronization parameter is input to the third sample and hold circuit, an output of the third voltage controlled oscillator provides an input to the fourth sample and hold circuit, an output of the fourth voltage controlled oscillator provides an input to the third sample and hold circuit, and the fourth voltage controlled oscillator outputs the copy of the key stream.

5. The system recited in Claim 4 wherein the receiving chaotic circuit comprises:

a hard limiting circuit for receiving the copy of the key stream from the third voltage controlled oscillator and for converting it to selected fixed values;

a sample and hold circuit for sampling the hard limited output of the hard limiting circuit at a fixed frequency to produce a sampled random signal; and

an analog multiplier circuit for multiplying the cipherwave with the sampled random signal to recover the information signal.

6. A chaos privacy method for use in communicating an analog information signal, the method comprising the steps of:

generating a random key stream using a chaotic circuit;

processing analog information signals and the random key stream to generate a cipherwave that has a uniform probability density for all information signals, and random key streams;

transmitting the cipherwave and a public key over a communication channel;

receiving the cipherwave, and public key;

synchronizing to the public key using a chaotic circuit to produce a copy of the random key stream; and

processing the cipherwave and the copy of the random key stream to reconstruct the analog information signal.

7. The method recited in Claim 6 wherein the cipherwave is generated by multiplying the information signals i(by the random key stream.

8. The method recited in Claim 6 wherein the information signal is generated by multiplying the cipherwave by the random key stream.